

CLAIMS

What is claimed is:

1. A method for extending and grouping actions and permissions for authorization of a requesting user to access or use a requested protected system resource in a computer system, said method comprising the steps of:
 - providing an access control policy associated with said requested protected system resource, said access control policy containing a permission list of permitted identities for use of said protected system resource, said permission list containing at least one action group tag and associated action indicators;
 - evaluating said permission list according to a specific permission definition associated with said action group tag, said permission definition providing a correlation between permissible actions and members of a set of action indicators; and
 - granting authorization to perform actions on said requested protected system resource to said requesting user if said access control policy permission list includes an appropriate action indicator correlated to an action group tag.
2. The method as set forth in Claim 1 further comprising providing in an access control policy permission list a plurality of action group tags, each action group tag having one or more associated action indicators, such that resultant granting of authorization to act on said requested protected object is completed if the requested action is allowed by any of the associated action indicators of any of the action groups.

3. The method as set forth in Claim 2 further comprising reusing action group permission indicators among action groups such that a finite list of action group permission indicators may be used to control a maximum number of unique permissions equal to the product of the number of unique allowable permission group indicators multiplied by a maximum number of allowable action group tags.
4. A method for managing permission indicators for computer system protected objects comprising the steps of:
- providing a plurality of permission indicator containers in an Access Control List;
 - 10 associating a first set of permission indicators with a primary permission indicator container; and
 - associating one or more additional sets of permission indicators with additional permission indicator containers such that permission indicators may be categorized and grouped logically to facilitate efficient and effective management of security policy.
- 15 5. The method as set forth in Claim 4 wherein said step of providing a first set of permission indicators comprises providing at least one other (additional) permission indicator set having equivalent permission indicators to said first set such that permission indicators may be assigned unique permissive control according to a permission indicator container with which they are associated.

6. The method as set forth in Claim 5 wherein said step of providing an equivalent set of permission indicators comprises providing the characters "a" through "z" and "A" through "Z" as permission indicators.

7. The method as set forth in Claim 5 further comprising associating an action
5 group tag with a permission indicator container.

8. The method as set forth in Claim 7 further comprising the step of providing an action group tag with an associated list of permission indicators in an Access Control List entry.

9. A computer readable medium encoded with software or extending and
10 grouping actions and permissions for authorization of a requesting user to access or use a requested protected system resource in a computer system, said software when executed causing a computer to perform the steps of:

providing an access control policy associated with said requested protected system resource, said access control policy containing a permission list of permitted
15 identities for use of said protected system resource, said permission list containing at least one action group tag and associated action indicators;

evaluating said permission list according to a specific permission definition associated with said action group tag, said permission definition providing a correlation between members of a set of action indicators; and

granting authorization to perform actions on said requested protected system resource to said requesting user if said access control policy permission list includes an appropriate action indicator correlated to an action group tag.

10. The computer readable medium as set forth in Claim 9 further comprising
5 software for providing in an access control policy permission list a plurality of action group tags, each action group tag having one or more associated action indicators, such that resultant granting of authorization to act on said requested protected object is completed if the requested action is allowed by any of the associated action indicators of any of the action groups.

10 11. The computer readable medium as set forth in Claim 10 further comprising software for reusing action group indicators among action groups.

12. A computer readable medium encoded with software for managing permission indicators for computer system protected objects, said software when executed causing a computer to perform the steps of:

15 providing a plurality of permission indicator containers in an Access Control List;
associating a first set of permission indicators with a primary permission indicator container; and

associating one or more additional sets of permission indicators with additional permission indicator containers such that permission indicators may be categorized and grouped logically to facilitate efficient and effective management of security policy.

13. The computer readable medium as set forth in Claim 12 wherein said software
5 for providing a first set of permission indicators comprises software for providing permission indicators which are equivalent to at least one other (additional) permission indicators such that permission indicators may be assigned unique permissive control according to a permission indicator container with which they are associated.

14. The computer readable medium as set forth in Claim 13 wherein said software
10 for providing equivalent permission indicators comprises software for providing a set of permission indicators including the characters "a" through "z" and "A" through "Z".

15. The computer readable mediums set forth in Claim 12 further comprising software for associating an action group tag with a permission indicator container.

16. The computer readable medium as set forth in Claim 15 further comprising
15 software for providing an action group tag with an associated list of permission indicators in an Access Control List entry.

17. An authorization system for extending and grouping actions and permissions for authorization of a requesting user to access or use a requested protected system resource in a computer system, said system comprising:

an access control policy associated with said requested protected system resource, said access control policy having a permission list of permitted identities for use of said protected system resource, and said permission list having at least one action group tag and associated action indicators;

a permission list evaluator for evaluating an access control policy permission list according to a specific permission definition associated with said action group tag, said permission definition providing a correlation between members of a set of action indicators; and

an authorization grantor adapted to grant authorization to perform actions on said requested protected system resource to said requesting user if said access control policy permission list includes an appropriate action indicator correlated to an action group tag.

18. The system as set forth in Claim 7 further wherein said access control policy permission list comprises a plurality of action group tags, each action group tag having one or more associated action indicators, such that resultant granting of authorization to act on said requested protected object is completed if the requested action is allowed by any of the associated action indicators of any of the action groups.

19. The system as set forth in Claim 8 wherein said action group indicators are reusable across action groups such that each action group may define a unique implementation of each reusable action group indicator.

20. A system for managing permission indicators for computer system protected
5 objects comprising:

a plurality of permission indicator containers for an Access Control List;

a first set of permission indicators associated with a primary permission
indicator container; and

one or more additional sets of permission indicators associated with additional
10 permission indicator containers such that permission indicators are categorized and
grouped logically to facilitate efficient and effective management of security policy.

21. The system as set forth in Claim 20 wherein said a first set of permission
indicators and at least one other (additional) permission indicator set are equivalent
permission indicators such that permission indicators are assigned unique permissive
15 control according to the permission indicator container with which they are associated.

22. The system as set forth in Claim 21 wherein said equivalent set of permission
indicators comprises the characters "a" through "z" and "A" through "Z".

23. The system as set forth in Claim 20 further comprising an action group tag associated with a permission indicator container.

24. The system as set forth in Claim 23 further comprising an action group tag associated with a list of permission indicators in an Access Control List entry.